IT Unit 3 Alex Hudson

Topic 1

# Organisations & Data Management Alex Hudson

**Protecting valuable data, p 57**

1. **Why is it important that stored data is kept secure?** Keeping data secure allows It to keep its integrity. Data that isn’t secure can be accessed by unwanted users, hackers and people with interests to manipulate the data for their own advantage.
2. **What are the 2 types of controls that can protect data?** Having a firewall can prevent many unwanted things/people from entering your network, such as viruses, unwanted users and access. Encrypting your data with tools and creating a special access key, which will enable you to access the data.

**Measures to protect data:**

**Physical equipment controls include zoned security strategies, barrier techniques and biometrics.**

**A What is meant by biometrics and what is it’s advantage as a means of protecting data?**

1. **Backing up**
   1. **What are the 3 types of backing up?** Full back up, incremental and differential back up.
   2. **List some backup options?** You can back up your data to an external hard drive, or upload it to a cloud space such as the Google Drive or Apple’s ICloud.
2. **Electrical protection**
   1. **What is the role of a UPS?** An Uninterruptable power supply can prevent power loss to servers, computers etc. Which all of these leads to the loss of important data.
3. **Usernames & passwords**
   1. **What are the characteristics of a good password?** Minimum eight characters long, doesn’t contain your name, not a complete word and uses a mix of upper/lower case, numbers and symbols.
   2. **What is the role of access logs, audit trails and access restrictions?** These can all restrict user access to certain commands or programs. Access logs allow company security teams determine which users have accessed what and the time they did it.
4. **Systems security software**
   1. **What types of security software should organisations run?** Any organisation, large or small, should use a Firewall- this can prevent any unwanted users and data entering the network
   2. **Explain the nature of malware and phishing software:** Malware and Phishing software target users to gain access to their data, programs, password and anything private. They typically are installed due to clicking on a spam email, visiting a dangerous site or installing a unscanned program. Having security scanners can prevent these installing.
   3. **Explain the nature of a firewall?** A firewall routes all internet usage both in and out of a network and checks it for viruses etc. It also has many settings which can restrict user’s access to the server and which users are actually allowed on the network.
5. **Encryption**
   1. **What does encryption involve?** Encryption involves using a security key to change data into a unreadable, not decodable language- the only person/s which can access the data are the ones with the security key.
   2. **What is hashing?** The transformation of a string of characters into a shorter fixed-length value or key that represents the original string.